Published and Copyright (c) 1999 - 2008
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1041 10/10/08

~ Unbreakable Encryption ~ People Are Talking! ~ New Apple Laptops!
~ Operation Cyberslam! ~ Bullying Kept Secret! ~ Pol Spam Surges!
~ Identifying Safe Sites ~ Facing "Clickjacking"! ~ OpenOffice 3.0 Soon!

~ Gmail’s Mail Goggles! ~ Fake YouTube Pages! ~ Zoho Goes Public!

-* Palin Email Hacker Indicted! *-
-* Tiny Flash Drives Improve Security! *-
-* SEC Probes Fake Jobs Heart Attack Posting! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

Well, as you’re all probably aware (and if you’re not, you’re living under a huge rock!), the world’s economic woes are worsening every day. No one knows where this is all going, but I have to think that things are going to get much worse before we see any real improvement. And if and when it’s discovered who is to blame, I really hope that a stack of books is thrown at all who are responsible! There’s plenty of blame to go around, I’m sure!

Personally, and I’m probably speaking for many, the pain is being felt at home. It’s bad enough that people are doing what they can to make ends meet these days, but now retirement savings are being threatened. In just this calendar year, my wife and I have lost thousands of dollars from our retirement fund. Not a good thing when only one of us has a real job. And my "seasonal" job will likely end within a few weeks. I’ve been looking around for something serious for quite some time, with no luck. Now I’m hoping to find something - almost anything - to help stem the financial blood-letting. We’ll see how that goes.

So, let’s move on to this week’s issue. The least we can do here is divert some of the painful economic news for a little while!

Until next time...

=~=~=~=

PEOPLE ARE TALKING
compiled by Joe Mirando
joe@atarinews.org

Hidi ho friends and neighbors. Another week has come and gone, and we’re mired even deeper in this financial mess.

I’m not going to go off on a rant about it, but I WOULD like to say that we’re NOT heading into another Great Depression. A friend replied to me, "Well 60 percent of the country believes we’re headed for a depression!"

"Yeah," I replied, "but I’m not worried about what they think... 60

percent of them also think The Flintstones was based on a true story."

Anyway, times are going to get tough, no doubt. We're headed for some rocky road ahead. And it won't be enough to simply scream, "But we're Americans!" because the entire world is going to feel this recession. And, quite frankly, they're not going to give a damn about YOUR nationality... they're going to be too busy giving a damn about their own situations.

One of the responsibilities of being a citizen of the last remaining global superpower is keeping the finance system stable. We've failed at that. We've failed miserably at it and, no matter how bad it gets here, there are other countries where it's going to be worse. People are going to die because of it.

Bail-outs? Rescues? Call 'em what you want, buddy, but the bottom line is still that they're expensive. Right now I don't care who's fault this mess is... we'll be able to place blame later... and extract pounds and pounds of flesh as necessary, but helping a company (not an industry, but a single company, mind you) by supplying them with tens of billions of dollars a week before they throw themselves a party and a week AFTER having been 'helped' with many tens of billions of dollars is just insane. Put them in receivership. If you want to make the federal government the conservator, that's fine, but they need to be answerable for their deeds, and for the 'gutting' of institutions and industries for the benefit of a few at the top.

Some have complained about the government assistance being equivalent to "buying high and selling low", and it's true that this is going to be a costly endeavor, but I just don't cotton to the idea of the government BUYING shares of these institutions. We've got enough problems now with separation of church and state and gun control and whatever else... we don't need to worry about the government changing the rules so that their 'businesses' make a profit for them. THAT would end up being a much larger bill in the end. And that's pretty much where we'd end up taking it.. in the end.

To be honest, I don't know that anything is going to both get us out of trouble and allow us to fix the system. Perhaps the only thing that'll fix the system is to change definitions and call a ball a strike, as it were. But we've got to try. There are just too many people's lives at stake. Too many people, and too many generations.

Well, that's enough of that. Let's get to the news, hints, tips and info available from the UseNet.

From the comp.sys.atari.st NewsGroup

Peter Slegg asks for help with his Milan Keyboard:

"Something weird has started happening with my Milan keyboard.

Last week I was having problems getting some keys to respond. I assumed it was the batteries in the wireless keyboard but the LEDs on the receiver puck were flashing every time I tapped a key. I changed the batteries anyway.

It has happened intermittently since but today it was working fine as I was using Texel. Then it suddenly stopped responding to lots of keys, particularly up, down, left right but Shift-up, down, left and right still worked.

It is fine in other apps (I'm using Everest now) but if I restart Texel it behaves oddly again."

Michael Schwingen asks Peter:

"Does this still happen if you remove the mouse?

I have seen erratic keyboard/mouse behavior when the +5V supply for the PS/2 ports (keyboard and mouse) is broken: if a device draws too much current, a PCB trace may blow. In that case, the +5V supply to both ports is broken, and keyboard/mouse get their power only from the pullup resistors on the data lines. If this works depends on the exact model of keyboard/mouse, and usually it works better when only one device is plugged in.

Anyway, you should try:
- a different keyboard/mouse, preferably a non-wireless model
- measuring the +5V on either port when both keyboard and mouse are plugged in

If the +5V supply is faulty, this can be fixed by soldering a small wire on the PCB."

Jo Even Skarstein adds:

"Have you tried with a different keyboard? Have you tried Texel in TOS (I guess you're still using MiNT)?"

There's no reply yet, but it's an interesting problem, so we'll check back next week and see what happens.

In the meantime, let's take a look at what 'Phil' was talking about with getting ethernet access with his NetUSBee:

"I've got a Netusbee connecting my 4mb Mega-STe to my PC.

I've connected the Ethernet cable from the Netus to my Netgear router. My ST has an IP address 192.168.02. I've tried pinging my ST from my PC and this works.

So far, so good.

Now the dodgy bit. Can anyone give me simple step of how to transfer files between the two ? I've tried FTPing 192.168.02 from my PC, no success. I then tried using Litchi but again I'm not sure what to do.

My MSTE is TOS only, is there a solution for this... or must I use Mint?

Any help appreciated.... had my Netus for over a year and not used it yet (flooded house problems!)"

Mike Freeman tells Grazey:

"First off, IP's should have 4 numbers, not 3. My guess is the IP is actually 192.168.0.2, *not* 192.168.02 (unless this was a typo)."

This [the solution] depends on what drivers and TCP/IP stack you have for your computer. If NetUSBee comes with a STiK/STing driver, you should be ok with TOS and those programs. If it only comes with a MintNet driver, you'll have to use Mint (it is possible to have a minimal Mint setup with MintNet on a slim system), or it might even work with Magic if you have that and MagicNet. I've not used a NetUSBee, so I can't say what drivers it needs. As for networking, once the drivers are running properly, setup is pretty much system independent, and I could help you with that end."

Phil tells Mike:

"Yes, just to clarify....

Firstly my ST is 192.168.0.2 (missed a 0 out there)
I have Sting up and running, I followed the guide here :-
http://hardware.atari.org/manuals/netsting.htm

So as I mentioned by PC can 'ping' my ST. This works under normal TOS.

As for FTP servers.. I guess this maybe the *slight* problem ;) So I need a FTP server set up on my PC..... this is were I need help I think, plus easy steps on the ST side of things to connect to my PC (or vice versa)....

I must admit when I bought the NetusBee I thought it would be similar to PC2Amiga were things ran in the background (TSR) and the PC or ST drive showed up on each machine.. .but we can all dream."

David Wade jumps in and adds:

"Sorry but the brain fades. I am sure there is a background FTP server. I think the one I used came from here:-

http://www.ettnet.se/~dlanor/sting/html/file.htm

And I used that with a windows graphical FTP client, but again I forget which one...

.. arrggh but I do remember I tried a number before I got a pair that worked well together.,..."

Derryck Croker adds his thoughts:

"It might not matter so much which end is the server, and which the client.

So if you decide that the PC is to be the server, then you'll probably want to give it a fixed IP address. Ask again if you need help for this.

Then, armed with whatever ST ftp client, you will know what address to type into it.

There is a solution for this, but IIRC you need to be running MagiC (or maybe MiNT, just in case anyone is about to jump up and down!)"

Edward Baiz adds:

"I have done this many times with great success using the FTP protocol. You first have to run a ftp server program on either machine. Get it up and running and then run a ftp program on the other computer and set it to the address of the other computer. The file should come up and you can then either download or upload the files you want"

Guillaume Tello comes by and adds this little tidbit:

"Try to run a FTP client on the ST with TYPSoft FTP server running on the PC (http://en.typsoft.com// a free program)."

Well folks, that's it for this week, tune in again next week, same time, same station, and be ready to listen to what they are saying when...

PEOPLE ARE TALKING

=~=~=~=

->In This Week's Gaming Section - More Wiis This Holiday?
"""""""""""""""""""""""""""""""" NBA 2K9 Ships!
A New Mind Game!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Nintendo Promises More Wiis This Holiday

Nintendo is promising consumers that there will be a larger supply of its Wii video game machines this holiday season.

The Wii has been in short supply, especially during the last two holiday seasons.

Nintendo has increased production to try to keep up with demand. It says it will increase shipments of the Wii between October and December.

It’s also increasing shipments of its portable Nintendo DS device.

NBA 2K9 Ships For Xbox 360, Playstation 3, and Playstation 2

2K Sports, the sports publishing label of Take-Two Interactive Software, Inc., announced Tuesday that the highly anticipated basketball title, NBA 2K9, is now available in retail stores for the Xbox 360 video game and entertainment system from Microsoft, and Playstation 3 and PlayStation 2 computer entertainment systems. NBA 2K9 provides unmatched attention to detail this season with even more signature style animations, deeper franchise mode, adaptive AI for smarter gameplay, and innovative online features including Team Up for true online 5-on-5 matches, and Living Rosters for the most up-to-date player

"Without question, NBA 2K9 is the most complete and realistic basketball simulation experience we have delivered to date," said Greg Thomas, senior vice president of sports development at 2K. "Not only did we perfect all the Signature Styles for each individual player and greatly enhance our broadcast presentation with 2K-HD, more importantly, the Adaptive AI plays an incredibly smarter basketball game this year than ever before, The Association 2.0 will be the most robust and accessible franchise mode of any sports title available, and our new and innovative online features with Team Up and Living Rosters will forever change the way basketball video games are played. It does not get any more real this season than with NBA 2K9."

NBA 2K9, the latest edition of NBA 2K and the #1 selling current gen basketball video game that has also been the #1 rated NBA simulation for seven years in a row, is back for its 10th season. NBA 2K9 is the premier basketball game for serious players, and will deliver the most realistic and feature-rich simulation experience ever available in the NBA 2K franchise - from gameplay and graphics to presentation and online features. If it happens during the regular NBA season, it will happen in NBA 2K9.

Fans can also now register online for The Other Season, a unique online fantasy league where roles are reversed and NBA 2K9 gamers get to play for real life NBA superstars who are participating as The Other Season fantasy team owners. Online gamers playing exclusively on Xbox LIVE online entertainment network and PlayStation Network will have the exciting opportunity to be drafted onto one of the NBA superstars NBA 2K9 fantasy teams. For more information on The Other Season and official rules, please visit http://www.theotherseason.com.

NBA 2K9 is rated E for Everyone by the ESRB and now available for Xbox 360, and the PlayStation 3 and PlayStation 2 systems. A Windows PC version will be available on October 21. For more information about NBA 2K9, please visit http://www.2ksports.com/games/nba2k9.

New Video Game Literally A Mind Game

Willpower is set to replace fast fingers in a new video game in which players move characters through a headset that monitors their brain waves.

California-based NeuroSky Inc. showed off the new headset - named Mindset - at the Tokyo Game Show, the industry's biggest exhibition which opened near the Japanese capital Thursday.

The Mindset monitors whether the player is focused or relaxed and accordingly moves the character on a personal computer.

"We brought this to the game show as a new interface, a new platform for game creators," NeuroSky managing director Kikuo Ito told AFP.

Children's games using the system will hit the US market next year, Ito said.

"We are exploring the use of brain waves in the game industry because games are fun and so close to people," he said.

"Once people get used to the idea of using brain waves for various applications, I hope we will see various products using this technology," he said.

In distance learning courses, for example, teachers could monitor whether students were attentive, Ito said.

Train drivers and motorists could use it to judge their stress levels and alertness, Ito added.

Japan's Keio University put similar technology to use this year to let a paralysed man take a virtual stroll on the popular Second Life website, with the machine reading what he wanted to do with his immobile legs.

NeuroSky said the Mindset could help people with other types of disabilities.

"For people with difficulty speaking, this can be a tool for communication," Ito said.

Ito was hopeful that the technology would eventually go on sale outside the United States. Prices have not been announced.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

SEC Probes Posting About Steve Jobs Heart Attack

On Friday a report that Apple CEO Steve Jobs had suffered a heart attack and was rushed to the hospital spawned a frenzy in Apple's stock. Now the Securities and Exchange Commission has launched an investigation into whether the false report was an effort to hurt the company's stock, according to CNN spokesperson Jennifer Martin.

Apple’s shares plunged Friday from $106.50 to $94.65 after a "citizen’s journal" report was posted on CNN’s iReport Web site.

The report said "Steve Jobs was rushed to the ER just a few hours ago after suffering a major heart attack. I have an insider who tells me that paramedics were called after Steve claimed to be suffering from severe chest pains and shortness of breath. My source has opted to remain anonymous, but he is quite reliable. I haven’t seen anything about this anywhere else yet, and as of right now, I have no further information, so I thought this would be a good place to start. If anyone else has more information, please share it."

iReport is CNN’s public journalism Web site, which allows users to post videos and photos showing news from their local towns. iReport was launched in 2006 and was bought by CNN last January and relaunched in March.

The Securities and Exchange Commission’s spokesperson, John Heine, said staff members are not authorized to confirm or deny whether the SEC "is investigating or not investigating" a company. But Martin said the company has been contacted by the SEC looking for information regarding the person who posted the message.

"The SEC has contacted iReport.com and we are certainly cooperating with them," Martin told us in a phone interview. "The report was taken off (the Web site) on Friday morning and the user’s, who submitted that report, account was canceled."

Apple issued a statement Friday denying the report that Jobs had a heart attack and Martin said the two companies have been in contact since.

Despite the false posting about Jobs, CNN Worldwide has no plans to make any changes to iReport.com, according to Martin.

"iReport in the spirit of it is unedited and uncensored," she said. "We want to create a community where users can go to and submit and upload user-generated content that they want to. ... We don’t plan on making any changes to iReport.com. If you go to [the] communications guidelines, it makes it clear that certain content is not welcomed on the site."

CNN uses a percentage of the content provided by users. In fact, CNN.com or CNN News ran 1,500 stories from the 21,000 user-generated stories posted to iReport.com last month, according to CNN.

"If any of that content is used in a CNN platform, it is fully vetted first," Martin said.

This isn’t the first time false news has hit the Web regarding Jobs’ health, which has been closely watched by the world ever since the executive said he had a rare form of pancreatic cancer that is more curable than other forms of pancreatic cancer.

Last month, Bloomberg News mistakenly ran Jobs’ obituary. It is a common practice for news outlets to have prepared obituaries for high-level business executives.

Palin Email Hacker Indicted by Grand Jury

A 20-year-old college student was indicted Tuesday by a federal grand jury in Tennessee for allegedly hacking into the Yahoo e-mail account of Republican vice presidential candidate and Alaska governor Sarah Palin.

David C. Kernell, a student at the University of Tennessee and the son of Tennessee state Rep. Mike Kernell, a Democrat, turned himself in to authorities on Tuesday and will be arraigned Wednesday before Judge C. Clifford Shirley.

If convicted, Kernell faces up to five years in prison, a $250,000 fine, and three years of supervised release. He is accused of gaining unlawful access to stored communications and obtaining information from a protected computer via interstate communication.

Kernell, who went by the Internet name of "rubico" or "rubico10", is accused of hacking into Palin’s "gov.palin@yahoo.com" e-mail account on September 16 by successfully navigating Yahoo’s password recovery system.

Palin’s e-mail address was revealed in several news stories around September 10, according to the indictment.

Palin had come under fire for allegedly using her personal Yahoo account to conduct state business, a move that could run afoul of transparency rules governing public officials.

Yahoo e-mail users who want to recover their passwords are required to provide their e-mail addresses, ZIP code, and date of birth. They must then answer a security question, which in Palin’s case was "Where did you meet your spouse?"

Any of the 40 million people who watched Palin’s GOP convention acceptance speech knew that she met her husband Todd in high school in her hometown of Wasilla, Alaska. It would not take a seasoned hacker to eventually land on the correct wording "Wasilla High" and gain access to Palin’s account.

Kernell cracked the code, changed the governor’s password to "popcorn" and then posted some of the account’s contents on hacker message board 4Chan, including personal e-mails, family photos, and Palin’s contact list.

The account has since been deleted.

"Cyber crime is the FBI’s top criminal investigative priority. We would like to thank all of the internet service providers and others who partnered with us to bring this matter to a quick and successful resolution." Richard Lambert, a special agent in charge with the FBI’s Knoxville Field Division, said in a statement.

The FBI searched Kernell’s apartment in late September, but a federal grand jury failed to return an indictment at the time.

Two Europeans Indicted Over U.S. Cyberattacks

Two Europeans, one of whom is English, have been indicted by a U.S. federal grand jury in connection with a 2003 distributed denial-of-service attack that is the focus of a major FBI investigation.

The two men, who are not in custody, were indicted as part of the FBI's Operation Cyberslam, initiated in 2003 following a series of crippling distributed denial-of-service, or DDoS, attacks on a large Los Angeles vendor of digital recorders. The attacks effectively knocked that business offline, along with other private and government bodies, for two weeks, resulting in losses ranging from $200,000 to more than $1 million, according to the FBI.

Operation Cyberslam is the first successful investigation of a large-scale DDoS used for a commercial purpose in the United States, the FBI said.

In 2004, two U.S. residents were charged with masterminding the attacks. The two Europeans indicted last week are accused of carrying out the attacks, and they face up to 15 years in prison, if convicted on charges of conspiracy and intentionally damaging a computer system, according to the U.S. Department of Justice.

Lee Graham Walker, 24, of Bleys Bolton, England, was indicted on Thursday, along with a German 25-year-old named Axel Gembe. Gembe is believed to be the programmer behind Agobot, a well-known worm used to create botnets that can be used in DDoS attacks or for other purposes, such as relaying junk e-mail.

The attacks were allegedly ordered by Saad Echouafni, a native of Morocco who was the owner of Orbit Communications. Paul Ashley, a business associate of Echouafni, was then responsible for contacting Walker and Gembe to carry out the attack, the Justice Department said. Ashley pleaded guilty in 2004 and has already served two years in an Ohio prison for his part in the conspiracy.

Echouafni, also indicted in 2004, is being sought by the FBI, which said he should be considered armed and dangerous.

Walker and Gembe allegedly used a botnet they had created together to carry out the attacks. According to the indictment, the two arranged the attacks over Internet Relay Chat (IRC), also using IRC to discuss ways of making their botnet code more damaging to Web sites.

The particular technique used in the attack was allegedly used to direct a flood of synchronization packets to the target Web sites. The botnet used was also capable of directing large amounts of malicious HTTP traffic, according to the Justice Department.

Tiny Flash Drives Improve Their Security

Flash memory drives, the size of your thumb, are dirt cheap and offer gigabytes of storage. It's tempting to fill one of them with important computer files, clip it to a key chain and hit the road.

But what if you lose it while fumbling for change at Starbucks and the hacker in the corner finds it? This is not a good thing.

That’s where a new breed of flash drives comes in - chock full of military-strength encryption and passwords and keypad combinations that must be entered before the data can be accessed.

I put a few secure flash drive solutions to the test: Take Anywhere’s Pocket Safe ($59.95), the IronKey ($149) and TrueCrypt, a free software program that works with any USB flash drive.

Each had its strengths and limitations, but I liked the IronKey unit best, with its built-in Firefox browser, large storage space and powerful password protections.

Setting up my 4-gigabyte, brushed-metal IronKey drive was pretty painless. After putting it in a USB slot on my home PC, I was asked to create a user name and password before I could access any of the storage space or other features. (Among those extra features: You can create an encrypted backup of the IronKey’s contents on a PC desktop.)

Then, every time you plug the IronKey into a computer, a control panel appears on the screen to ask for the password again. No password, no reading or tinkering with the drive’s contents. In fact, you have to be careful, because if you enter the wrong password 10 times in a row the unit permanently deletes all of your data and is no longer usable. You can’t even reformat it. That’s tough love.

My favorite IronKey feature was the built-in Firefox browser. It let me take my favorite Web bookmarks and login information with me, along with my Web surfing cookies and site history. This means I left no trace of my Web browsing on the computers I plugged the IronKey into.

The IronKey works best with Windows XP, Linux and Mac OS X, according to the company.

Next up was the Pocket Safe (for Windows only), from Take Anywhere. The 1-gigabyte device sports a numerical keypad on its case. If you don’t remember the password you create, you won’t be able to launch the drive’s software control panel.

I picked a four-digit password, but there are two numbers for each of the five entry buttons on the keypad. So if my access code were 1-2-3-4, someone could guess it by keying in 0-3-2-5 or 1-2-2-4 or other shared-button combinations. This was disappointing.

Once I keyed in my correct password, a green light began to blink, telling me it was safe to insert the Pocket Safe drive into my USB port.

The Pocket Safe’s on-screen control panel features a column of icons down the left side, for categories of data such as financial accounts, Web site logins and vehicle records. This is handy for staying organized.

By default, Pocket Safe times out after 20 minutes of zero interactivity with the control panel, which got annoying. I had to go into the settings and beef it up to an hour.

TrueCrypt (for Windows 2000 and XP, Linux) is a piece of open-source software that promises to turn almost any USB flash drive into one Jason Bourne would be proud of. TrueCrypt creates and then hides a password-protected partition on the drive.

I installed the TrueCrypt application on my laptop and plugged in an old 512-megabyte flash drive, a giveaway from a tech convention. TrueCrypt let me choose between creating a file container on a portion of my flash drive (recommended for newbies) or encrypting the entire drive. Both methods worked flawlessly.

As a test, I plugged my TrueCrypt-encrypted flash drive into a PC that did not have the TrueCrypt application installed. I found the flash drive listed under "My Computer," but the PC recognized zero bytes of used space, and zero bytes of free space. Only installing TrueCrypt and knowing my password would uncloak my data. The method seems secure.

Beyond these three storage techniques, I also tried something else for people who want plug-in computer security: the $149 Yoggie Gatekeeper Pico. This unit looks like a flash drive but instead serves as a physical barrier of security for the laptop or desktop it’s plugged into. Instead of relying on installed firewall security on your PC, the Yoggie asks that you uninstall your security software and let the flash drive itself do the protecting.

Once the Yoggie management software was installed and launched on my PC, I couldn’t conduct any online activity unless the Yoggie was plugged in to the USB port. The makers of Yoggie say it’s better to block Internet virus and malware threats before they reach your physical PC, rather than depending on installed software to root them out once they’ve arrived.

It generally worked, although the Yoggie software was sluggish and the unit wasn’t always recognized by my PC. Sometimes the little blue lights on the Yoggie device blinked happily and let me proceed online, sometimes they didn’t. Even when it was working, the Yoggie took too long to be recognized by its own software companion.

Apple To Unveil New Or Updated Laptops

Apple Inc will unveil its updated laptops on October 14 and they may cost less, but analysts say the company’s drooping stock has already taken any change into account.

"I think it’s already factored into the stock. People have been expecting this announcement for well over a month," said Andy Hargreaves of Pacific Crest Securities in Oregon.

Apple enters the fourth quarter against a background of continuing headlines about falling stocks and failing banks, and a September in which retail sales dived beyond expectations.

At minimum, Apple will use the event at its Cupertino, California, headquarters to refresh its laptop line by updating to the latest chips and it may also offer new designs.

The Apple invitation said only: "The spotlight turns to notebooks." Occasionally, Apple unveils revolutionary new approaches at such events, but analysts shrugged when asked about the possibility.

"You won’t know that until the day of the event," said Tim Bajarin of Creative Strategies in Campbell, California.

Analysts also raised the possibility of a drop in the sticker price for laptops that now start at $1,099, more than twice the cost of the cheapest of the Window-based laptops.

Apple chief financial officer Peter Oppenheimer opened the door to speculation as long ago as July 21 during a discussion of the company's computer line.

The executive said the company introduces "new products that initially cost more because they deliver an entirely new level of value to the customer. Then we ride the cost curves down with value engineering and volume manufacturing, leaving us far ahead of our competitors."

Bajarin was cautious and stopped short of forecasting price cuts.

"It's a possibility. We don't know that for sure," he said.

He said Apple emphasizes design and functionality, "but clearly they have become more price conscious as they have become more competitive."

OpenOffice 3.0 To Launch

OpenOffice.org will host a launch party in Paris on October 13 to celebrate the eighth anniversary of OpenOffice and the release of version 3.0.

That day will hopefully mark the actual availability of the software as well; "[The] target date is now 13th or 14th of October," Charles Schulz wrote on the OpenOffice marketing blog on Oct. 2.

Meanwhile, OpenOffice 3.0 release candidate 4 is available via the organization's Web site as of Oct. 7. However, RC4 is not recommended for production use, as it is not the final product, OpenOffice.org said.

OpenOffice, intended to be a free, open-source alternative to Microsoft Office, released the beta version of 3.0 in May. OpenOffice 3.0 will feature a new Start Center, icons, and zoom control in the status bar, as well as support for the ".docx" file format used by Microsoft Office 2007. The release candidate also includes additional, technical updates, details of which are provided on the OpenOffice Web site.

The launch event will be sponsored by the Region Ile de France, Silicon Sentier, and OpenOffice, and will feature presentations by Jean-Paul Huchon, president of Region Ile de France, Louis Suarez-Potts, president of the OpenOffice.org Community Council, and Charles-H. Schulz, leader of the native-language confederation at OpenOffice.org.

The party is open to everyone, and registration is available online.

Earlier this year, versions of OpenOffice between 2.0 and 2.4 were affected by a vulnerability in the software's custom memory allocation routine. It was discovered by iDefense's VCP (vulnerability contributor program), which allows researchers to submit vulnerabilities and exploit code for money.

EU Scientists Launch New, ’Unbreakable’ Encryption System

A new encryption system, which its creators say is unbreakable, got its first test run Wednesday in Vienna, scientists from the European Union project SECOQC announced.

The successful demonstration, developed by the EU’s Development of a Global Network for Secure Communication based on Quantum Cryptography (SECOQC) paves the way for it to be used in ordinary communications networks.

"Potential users of this network, such as government agencies, financial institutions or companies with distributed subsidiaries, can encrypt their confidential communication with the highest level of security," said a SECOQC statement.

This kind of network should be commercialised within three years, said the project’s Austrian coordinator, Christian Monyk.

The technology works by sending streams of light particles, or photons - and that, say the scientists who created it, means it is entirely secure, as any eavesdropping would leave traces and immediately be detected.

Encrypted data, including a videoconference, was transmitted via standard optical fibre to six different centres, some as far as 82 kilometres (50 miles).

The demonstration took place during a three-day international conference in the Austrian capital to demonstrate the system.

Until now, quantum cryptography has been used simply to transmit information from one point to another, rather than as part of a network.

It is the result of four and half years of work by 41 partners, mostly universities and research centres, from 12 European countries.

Led by the Austrian Research Centers, the project was sponsored by one of the fathers of quantum physics, Anton Zeilinger from the University of Vienna.

Scientists from Austria, Belgium, Britain, Canada, Czech Republic, Denmark, France, Germany, Italy, Sweden and Switzerland all participated in the 11.4-million-euro SECOQC project.

Web Surfers Face Dangerous New Threat: ’Clickjacking’

Internet and Web browser security experts are sounding the alarm about a new type of malicious attack called "clickjacking," a technique that can be used to dupe Web surfers into revealing confidential information while clicking on seemingly innocuous Web pages. Among other things, a clickjacking attack can be used to take control of a computer’s Webcam and microphone without the knowledge of the user.

Clickjacking has been identified as a vulnerability for the Adobe Flash player, as well as for every major browser, including Firefox, Internet

Explorer, Opera, Safari and even the newly released Google Chrome.

"It is a very serious problem," said Giorgio Maone, the author of a widely praised free Firefox extension called NoScript, which blocks potentially malicious scripts from running in the Firefox browser.

"Clickjacking is a very simple attack to build, and now that the details are out, any script kid can try it successfully," Maone warned. "There's no estimate to the number of trap sites, and it's unlikely that we will see any credible report about the number of sites using this technique, because there are literally infinite ways to implement such an attack, therefore no signature-based scanning can detect it automatically."

The growing severity of the clickjacking problem was identified by Robert Hansen, CEO of SecTheory, and Jeremiah Grossman, CTO of WhiteHat Security. The two were scheduled to speak publicly about their discovery last month at the Open Web Application Security Project NYC AppSec conference in New York, but postponed their talk in order to give Adobe and browser companies a chance to come up with a solution.

Reacting quickly to the announcement, Adobe released a security advisory Tuesday, describing the threat as "critical" and instructing users on how to turn off Flash access to cameras and microphones.

"We have just posted a Security Advisory for Flash Player," wrote David Lenoe, Adobe's security program manager, on the Adobe security blog, "in response to recently published reports of a 'clickjacking' issue in multiple Web browsers that could allow an attacker to lure a Web browser user into unknowingly clicking on a link or dialog. This potential 'clickjacking' browser issue affects Adobe Flash Player's microphone and camera access dialog." Lenoe said a patch for Flash would be ready by the end of October.

Unfortunately, as Hansen and other researchers have pointed out repeatedly, Flash clickjacking is only one of the variants of this problem. In a lengthy blog posting about the issue, Hansen said that "there are multiple variants of clickjacking. Some of it requires cross-domain access, some don't. Some overlay entire pages over a page, some use iframes to get you to click on one spot. Some require JavaScript, some don't. Some variants use CSRF to preload data in forms, some don't. Clickjacking does not cover any one of these use cases, but rather all of them."

Hansen warned that it will be challenging to come up with a comprehensive solution to prevent the clickjack threat because of the nature of the code that underlies the Internet.

Maone agreed. "This problem comes from features which are integral to the modern Web as we know it," he said, "and especially from the ability of Web pages to embed arbitrary content from different sites, or to host little applications (applets) through plug-ins like Adobe Flash, Java or Microsoft Silverlight."

Maone predicted that a general browser fix won't be developed any time soon, since the real solution lies in developing a general consensus about changing existing Web standards in the various Internet standardization groups.

Firefox Plug-In Updated To Fight Clickjacking Attacks

Mozilla is doing its part in the battle against clickjacking. The open-source company is offering an updated plug-in for the Firefox browser that blocks what security researchers call one of the most dangerous problems on the Web.

Clickjacking occurs when a person browsing a Web site clicks on an invisible link that leads them to a malicious site without their knowledge. Some never realize it even happened. A design feature in HTML that lets Web sites embed content from other sites makes it possible, which means nearly everybody is vulnerable.

The Firefox add-on, NoScript, is a well-known security plug-in. It is used to block all sorts of content types within Web pages. It is not a security scanner in the sense that it does not scan content with any form of signature database to look for specific known threats. Rather, it is a tool that enables you to block certain types of content. An update to NoScript includes a feature dubbed ClearClick to combat clickjacking.

According to Fraser Howard, principal malware researcher at SophosLabs, the new feature in NoScript is specifically designed to combat the user-interface redress attacks known as clickjacking and should help. However, there is a potential downside.

"Enabling the feature will result in some degree of false positives," Howard warned. "This is not a criticism of the product; more a reminder that given the widespread legitimate use of similar techniques, some false positives are inevitable."

Of course, the NoScript add-on alone isn’t enough to solve the problem. That’s because it only covers Firefox. The other 70 percent of the browser market is still open to clickjacking.

"User discretion is still an important factor in the defense against these attacks, just like any other," Howard said. "The usual common-sense guidelines apply to this, just like other forms of malicious Web attack."

Security researchers expect other browsers to follow Mozilla and release some form of defense against clickjacking. In fact, Howard said some may already have this built in, though Mozilla has so far been the only one to announce it in the wake of the recent alerts about user-interface redress attacks.

"The problem is doing this without breaking sites and Web applications we have come to rely on," said Howard, noting that defending against clickjacking is a complex problem. "There is no silver bullet."

Web applications could also be targeted. Howard noted proof of concept demos he’s conducted that abuse the Web page Adobe uses to administer a user’s Flash security settings. In one proof of concept called "the clicking game," victims are encouraged to click in the right places to reconfigure the security settings that allow access to a Webcam or microphone.

In a similar way, Howard said, imagine an attack that woos victims to click on the necessary objects within their favorite Webmail application

to delete all their mail. There are numerous ways to envisage an attack targeting an application you are already authenticated to when you happen across a malicious page, he noted.

"The owners of those applications can take steps to eliminate or minimize risk. For example, Adobe added a simple block of JavaScript to prevent a site being able to frame in their security settings config page," Howard said. "Other fixes could be to ensure there are additional steps, such as a CAPTCHA [distorted image] or password, involved in any actions that are potentially dangerous."

Zoho Mail Goes Public With Offline Capabilities

Zoho Mail has emerged from its private beta-testing stage. Tapping functionality built into Google Gears, Zoho's Web-based e-mail application now sports a "setup offline" link at the top of the page that gives users offline e-mail access.

To operate Zoho Mail in offline mode, the user needs to have Google Gears installed in a Internet Explorer or Firefox browser, said Zoho cofounder and evangelist Raju Vegesna.

"We offer support for up to 5,000 e-mails currently and make them available to users as a download they can access when not online," Vegesna said. "You can also choose to download images and attachments to access in the offline mode."

One component of Zoho's product release is an e-mail add-on to the company's suite of productivity applications, Vegesna said. "If an individual, you'll get a free e-mail account with unlimited storage, and will be able to open e-mail from your other existing accounts as well," he said.

Any e-mail in the offline user's outbox will be sent as soon as an online connection is established, and any other changes the user has made while in offline mode will automatically synchronize with the online platform.

"I've got to say that I am really impressed," commented Brad Neuberg of the Google Gears team. "Offline is hard, especially with something like e-mail."

Zoho Mail automatically detects the user's connectivity status and switches to online and offline modes seamlessly, Vegesna said. "While offline, you can view your e-mails as you would normally," he added.

The application supports both the standard folders structure in Microsoft Outlook and the labels capability in Gmail. "We didn't want to decide what you should use - we wanted to give you a choice," Vegesna said.

The labels capability allows users to view e-mails as conversations, Vegesna noted. "In conversations, responses are listed hierarchically so that you can visually see who responded to whom," he said.

Additionally, Zoho Mail integrates a chat capability. "We understand that you spend most of the time in your e-mail app, so now you can chat

while you are in Zoho Mail," Vegesna said.

The other component of the company's new offering is Zoho Mail for businesses. "It is a replacement for Outlook and Microsoft Exchange Server," Vegesna said. "So if you have 300 employees and are looking for an e-mail server, you can bind your domain to Zoho Mail and we'll host your e-mails for your employees, each with their own e-mail address."

For enterprises with less than 10 employees, Zoho Mail for businesses is free. "We also have an office suite as well, and if less than 10 employees are involved, they can use all of these applications for free," Vegesna said.

Zoho's suite of productivity and collaboration applications also includes online word processing, spreadsheet, presentation, document management, wiki and notebook programs. "From the eleventh user on, the all-inclusive pricing is $50 per user per year," Vegesna said. "But if you are an individual, then all of these apps are free."

Additionally, Zoho Mail now features mobile support mobile for Apple's iPhone. "We built a mobile client that allows you to access your mail on the iPhone, and we soon plan to extend this to cover other devices like the Blackberry," Vegesna said.

Is This Site Safe For Your Kids? CyberPatrol Knows

Have you ever glanced over your child's shoulder at the computer screen only to see a URL that seems... weird?

Deviantart.com? What could that be? Something, well, deviant? The new free SiteCAT lookup service from parental control vendor CyberPatrol makes it easy to answer the question.

Just type in the URL at http://www.cyberpatrol.com/lookup.asp to learn how CyberPatrol categorizes the site.

It's not just a matter of good versus bad sites: CyberPatrol assigns 45 distinct categories. Nine categories are "blocked," among them Adult, Gambling, and XXX. Among the 36 "allowed" categories are innocuous ones such as Arts, Entertainment, and News. (That suspicious-sounding deviantart.com is correctly identified as an Arts site.) The "allowed" group also includes some you might consider mildly worrisome, like Chat, Lingerie, and Weapon Related. What you do about the answer is up to you--there's no actual blocking involved. Maybe you don't agree with the category assigned to a site? No problem! The results page includes a large panel for your comments.

The service is similar in some ways to SiteAdvisor and LinkScanner, both of which let you enter a URL and receive a rating. But CyberPatrol doesn't plan to expand its SiteCAT lookup service to mark up search results the way the other two do. It's just a simple way to find out about the sites your kids (or employees) visit.

Fake YouTube Pages Used To Spread Viruses

Savvy Internet users know that downloading unsolicited computer programs is one of the most dangerous things you can do online. It puts you at great risk for a virus or another time bomb from a hacker.

But even some sophisticated surfers could get taken in by a sneaky new attack in which criminals create fake YouTube pages - dead-on replicas of the real site - to push their malicious software and make it look like it’s safe stuff coming from a trusted source.

A program circulating online helps hackers build those fake pages. Users who follow an e-mail pointing them to one of the pages would see an error message that claims the video they want won’t play without installing new software first. That error message includes a link the hacker has provided to a malicious program, which delivers a virus.

Even worse: once the computer is infected, it’s simple for the hacker to silently redirect the victims to a real YouTube page to see videos they were hoping to see - and hide the crime.

"It’s spot-on accurate, and that is scary," said Jamz Yaneza, threat research manager for security software company Trend Micro Inc. "If I were watching YouTube videos all day I would probably click on this one."

The tactic itself isn’t new: There’s a constant push by criminals to build more convincing spoofs of legitimate sites to trick people into downloading harmful software. And the latest attacks don’t target any vulnerability in the YouTube site.

But it highlights the fact that criminals are getting better at creating bogus sites and developing so-called "social engineering" methods to fool people.

Fortunately, truly alert Internet users can still see the telltale warning signs with the fake YouTube pages. For one, the Web browser won’t show the real YouTube’s Internet address. And to even see the malicious page, you have to first follow a link that’s sent to you, which is often a tip-off that you should independently verify whether the site is legitimate.

Oops! Google Gmail Can Save You From Yourself

If you’ve ever hit the send button after writing an e-mail while under the influence only to feel that immediate pit in your stomach called regret, then a new Google feature may be just what you need.

The Internet search giant has added a feature to Gmail called Mail Goggles, which allows users to take a closer look at an e-mail while preventing the sending of messages to significant others, friends and bosses in the late hours of the night. The feature is only available at night and on the weekend, according to the Official Gmail Blog.

Jon Perlow, a Gmail engineer who wrote the code for Goggles, said he developed the feature after his own bad experiences in sending e-mail and text messages in the wee hours of the night.

"Sometimes I send messages I shouldn’t send like the time I told that girl I had a crush on her over text message. Or the time I sent that

late night e-mail to my ex-girlfriend that we should get back together," Perlow wrote. "Gmail can’t always prevent you from sending messages you might later regret, but today we’re launching a new Labs feature I wrote called Mail Goggles which may help."

"When you enable Mail Goggles, it will check that you’re really sure you want to send that late night Friday e-mail," Perlow added. "And what better way to check than by making you solve a few simple math problems after you click send to verify you’re in the right state of mind?"

Perlow isn’t joking. Users who activate Mail Goggles must first solve a group of simple math problems in a short period before hitting send. The simple math problems are a safeguard for those who may not be in the right state of mind to send e-mail.

Of course, Mail Goggles might not work for math geniuses who can solve problems while intoxicated or tired, or those who are determined to hit send.

Once Mail Goggles is activated, the user can adjust when it’s active in Gmail’s settings, under the Labs tab.

Gmail’s Lab launched in June as a way to allow software engineers to bring their ideas to life in an easy and fun manner, according to the company. The idea is that an engineer can go get a snack, think up an idea, write code for the idea, and use it as a Lab feature, said Product Manager Keith Coleman in a blog introducing the lab.

The lab also allows its users to provide feedback on new features and decide their fate.

There are nearly two dozen Lab features that have been developed for Gmail users. Some of the most popular, however, are Custom Label Colors, Superstars, Forgotten Attachment Detector, and Mark as Read Button.

So now it’s up to Gmail users to decide if they need to do a little math before hitting send.

Sinking Shares Could Make Yahoo A Target Again

When Yahoo Inc. co-founder and CEO Jerry Yang spurned Microsoft Corp.’s rich buyout offer this spring, he promised brighter days in Sunnyvale were just over the horizon.

Now the market collapse has helped drive Yahoo’s value to a fraction of what Microsoft originally bid. If Microsoft - or another buyer - were to float a new offer, the acquisition would come much cheaper, and Yahoo would likely be under even greater pressure to take it.

Matt Rosoff, an analyst for the independent research group Directions on Microsoft, said Microsoft is much less likely to bid for all of Yahoo this time. Its search engine, No. 2 to Google Inc.’s, would likely be Microsoft’s target.

Rosoff said Yahoo’s pummeled stock price leaves time on Microsoft’s side. The company can afford to throw money into its own Internet search operations and swoop in when Yahoo is finally strapped.

"I think they're looking at Yahoo as a rapidly declining asset," he said.

On Feb. 1, Microsoft tried to buy Yahoo for $31 per share, or $44.6 billion at the time, in a mixture of cash and stock. The offer marked a 62 percent premium to Yahoo's closing price of $19.18 the day before.

Microsoft later sweetened its bid to $33 per share, or $47.5 billion - an amount Yang and board chairman Roy Bostock said in May still undervalued Yahoo.

Since then, Yahoo's share price has been halved and analysts are seeing few bright spots as they slash expectations for Web display advertising, Yahoo's strength, in the coming quarters.

Microsoft's stock has been battered as well, but even at the shares' current level, Microsoft's original stock-and-cash bid for Yahoo would be worth about $37.1 billion to Yahoo shareholders. That's more twice Yahoo's current market value.

Having missed that opportunity, many Yahoo shareholders would love to see another one emerge now.

Mithras Capital, a Napa, Calif.-based investment fund that said it holds more than 1.9 million Yahoo shares, this week urged Microsoft to come back with an offer to buy just Yahoo's search business for $10.3 billion, a tactic that failed for the software maker in July.

"It is imperative for the Yahoo board to embrace this proposal as the best outcome for long-suffering Yahoo shareholders," Mithras' Mark Nelson wrote in a statement.

The bigger question is whether Microsoft is still interested, even though its plan to pour more resources into Web search and online advertising have not borne fruit. And given the lack of support for a deal among Yahoo executives and employees, regulatory uncertainty that will last at least through the November elections and the economic turmoil, a deal could simply take too long, Rosoff said, giving Google time to grow even stronger.

Kids Keep Parents in The Dark About Cyberbullying

Online bullying could be more pervasive than you think.

Three out of four teens were bullied online over the last year, according to a study released this week by psychologists at the University of California, Los Angeles. And while that number may seem high at the outset, only 1 in 10 of those kids told their parents or another adult about it, the study showed.

The anonymous Web-based study surveyed 1,454 kids between the ages of 12 and 17. Of those, 41 percent reported between one and three cyberbullying incidents during the year; 13 percent reported four to six incidents; and 19 percent reported seven or more. In other words, no longer are victims of bullying relegated to the geeks and nerds of yore when it comes to the Internet.

The psychologists published the results of their research in the September issue of the Journal of School Health.

Many teens neglected to tell their parents about the incidents because they believed they "need to learn to deal with it," according to the research. Others kept it to themselves because they feared that their parents would cut back on their Internet access.

"Many parents do not understand how vital the Internet is to their social lives," said Jaana Juvonen, lead study author and a professor of psychology and chair of UCLA's developmental psychology program. "Parents can take detrimental action with good intentions, such as trying to protect their children by not letting them use the Internet at all. That is not likely to help parent-teen relationships or the social lives of their children."

Juvonen said it's important that parents talk with their kids about bullying well before it happens, as well as look for changes in teens' behavior.

However, it's also equally important to teach children the importance of not becoming bullies themselves, is it not? Surely if bullying is this prevalent online, it's not always a one-sided affair.

Palin Wins 'Spam Debate,' As Does Obama

In a study released by Secure Computing on Friday, the amount of spam citing Gov. Sarah Palin topped her opponent, Sen. Joe Biden, by a ratio of 5 to 4 during the month of September. But in a top-of-the-ticket comparison, spam using the name of Sen. Barack Obama easily topped the use of his opponent, Sen. John McCain, by 6 to 1.

What does this say? That spammers are continuing to use the most provocative names and subjects as possible, to lure users into opening the source email. A "surge" of Obama spam was apparently timed for around Sept. 3, about the time of the Republican National Convention.

By comparison, news stories citing Obama or McCain favored McCain, 10 to 9. Web sites mentioning Obama outrank those that cite McCain, 3 to 2. But the spam associated with Sarah Palin is closer to the news stories or Web sites mentioning Palin, both of which outstrip Biden citations by 7 to 2.

And what do the spammers tie to the candidates' names? In the case of Obama, "Though the spam message content itself is nonsensical, the basic themes of the Obama email content does tend to revolve around the shallow factors that are espoused in the mainstream media as central campaign issues: race, disputes with Clinton, messianic oratory, and FOX news smears," Secure Computing wrote. "The McCain spam subjects are equally driven by shallow media propaganda, revolving around age and wealth."

Secure Computing also warned that October could see an uptick in spam and other phishing attempts mentioning either the banks which either were taken over or went under, such as Wachovia and Washington Mutual. In addition, there has been a rise in "gibberish spam," nonsensical messages that are either a glitch in the spammers' software or an

attempt to weed out nonfunctioning email addresses.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.